What is claimed is

1. A method comprising:

obtaining a portion of data to be analyzed to determine a network attack;

carrying out a data reduction on said portion to reduce said data portion to a reduced data portion in a repeatable manner; and

analyzing a plurality of said reduced data portions to detect common elements within said reduced data portion, said analyzing reviewing for common content indicative of a network attack.

2. A method as in claim 1, wherein said analyzing common content comprises determining frequently occurring sections of message information within said reduced data portion.

3. A method as in claim 1, wherein said analyzing common content comprises determining increasing number of sources and destinations that are sending and/or receiving within said portions.

4. A method as in claim 1, further comprising analyzing for the presence of a specified type of code within said data.

5. A method as in claim 2, further comprising after said analyzing determines said frequently occurring sections of message information, then carrying out an additional test on said frequently occurring sections of message information.

6. A method as in claim 5, wherein said additional test is a test to look for an increasing number of at least one of sources and destinations of said frequently occurring sections of message information.

7. A method as in claim 5, wherein said additional test includes a test to look for code within the frequently occurring sections.

8. A method as in claim 1, wherein said data reduction includes carrying out a hash function on said portion of data.

9. A method as in claim 2, wherein said determining frequently occurring sections is done by using at least first, second and third data reduction techniques on each said portion, to obtain at least first, second and third results, and to count said first, second and third results, and to establish frequently occurring sections when all of said at least first second and third results have a frequency of occurrence greater than a specified amount.

10. A method as in claim 1, wherein said portion of data at least includes a portion of the network payload.

11. A method as in claim 5, wherein said additional test comprises maintaining a first list of unassigned addresses; forming a second list of sources that have sent to addresses on said first list; and comparing a current source of a frequently occurring section to said second list.

12. A method as in claim 11, wherein said maintaining, and said forming, and said comparing, each comprise data reducing information in said first list and said second list.

13. A method as in claim 5, wherein said additional test comprises:

first monitoring a first content sent to a destination;

second monitoring a second content sent by said destination; and

determining a correlation between said first content and said second content as said additional test.

14. A method as in claim 13, wherein said first monitoring comprises monitoring multiple destinations, and said second monitoring comprises monitoring multiple destinations during a different time period than said first monitoring.

15. A method as in claim 14, wherein said first and second monitoring comprises data reducing information about said destinations, and storing at least one table about said data reduced information.

16. A method as in claim 10, wherein said portion of data further includes portion of a network header.

17. A method as in claim 11, wherein said portion of a network header is a port number indicating a service requested by a network packet.

18. A method as in claim 17, wherein said port number is a source port or a destination port.

19. A method as in claim 1, wherein said portion of data comprises a first subset of a network packet including payload and header and further comprising obtaining a second subset of the same network packet for subsequent analysis.

20. A method as in claim 1, further comprising forming a plurality of portions from each network packet, each of said plurality of portions comprising a specified subset of the network packet.

21. A method as in claim 1, further comprising forming a plurality of portions from each network packet, each of said plurality of portions comprising a continuous portion of payload, and information indicative of a port number indicating a service requested by a network packet..

22. A method as in claim 2, wherein said determining frequently occurring sections comprises:

taking a first hash function of said portion,

first maintaining a first counter, with a plurality of stages, and incrementing one of said stages based on said first hash function;

taking a second hash function of said portion; and

second maintaining a second counter, with a plurality of stages, and incrementing one of said stages of said second counter based on said second hash function.

23. A method as in claim 22, further comprising checking said one of said stages of said first counter and said one of said stages of said second counter against a threshold, and identifying said portion as frequent content only when both said one of said stages of said first counter and said one of said stages of said second counter are both above said threshold.

24. A method as in claim 23, further comprising adding frequent content to a specified frequent content buffer table.

25. A method as in claim 24, further comprising taking at least a third hash function of said portion, and incrementing a stage of at least the third counter based on said third hash function, where said identifying identify said portion as frequent content only when all of said stages of each of said first, second and third counters are each above said threshold.

26. A method as in claim 22, further comprising obtaining said portion by taking a first part of the message, and subsequently obtaining a new portion by taking a second part of the message.

27. A method as in claim 26, wherein at least one of said hash functions is an incremental hash function.

28. A method as in claim 3, wherein said data reduction comprises hashing at least one of the source or destination address, to form a hash value, first determining a unique number of said hash values, and second determining said one of source or destination numbers based on said first determining.

29. A method as in claim 28, wherein said counting further comprises scaling the hash value prior to said second determining.

30. A method as in claim 29, wherein said scaling comprises scaling by a first value during a first counting session, and scaling by a second value during a second measurment interval.

31. A method as in claim 7, wherein said detecting code comprises looking for a first valid opcode at a first location, based on said first valid opcode, determining a second location representing an offset of said first valid opcode, and looking for a second valid opcode at said second location.

32. A method as in claim 31, further comprising establishing the portion as including code when a predetermined number of valid opcodes are found at proper distances.

33. A method as in claim 1, further comprising, determining a list of first computers that are susceptible to a specified attack, and monitoring only messages

directed to said first computers for said specified attack.

34. The method of claim 33 where said monitoring comprises checking for a message that attempts to exploit a known vulnerability to which a computer is vulnerable, as said specified attack.

35. A method as in claim 34, wherein said checking comprises checking for a field that is longer than a specified length.

36. An apparatus comprising:

a signature generator, having a connection to a network, to obtain a portion of data from the network, operating to carry out a data reduction on said data portion to reduce said data portion to a reduced data portion in a repeatable manner; and

a memory, storing said reduced data portions; and

wherein said signature generator also operates to detect common elements within said reduced data portion, said analyzing reviewing for common content indicative of a network attack.

37. An apparatus as in claim 28, wherein said signature generator determining frequently occurring sections of message information within said reduced data portion.

38. An apparatus as in claim 36, wherein said memory stores information indicative of at least one of a number of sources sending the common content, and/or destinations that are receiving the common content, and said signature generator determines whether said number is increasing.

39. An apparatus as in claim 36, wherein said signature generator also analyzes for the presence of a specified type of code within said data portion.

40. An apparatus as in claim 37, further comprising a module that carries out an additional test on said frequently occurring sections of message information after said signature generator determines frequently occurring sections of message information.

41. An apparatus as in claim 40, wherein said additional test is a test to look for an increasing number of at least one of sources and destinations of said

frequently occurring sections of message information.

42. An apparatus as in claim 41, wherein said module is a module to look for code within the frequently occurring sections.

43. An apparatus as in claim 36, wherein said data reduction by said signature generator includes carrying out a hash function on said portion of data.

44. An apparatus as in claim 37, wherein said determining frequently occurring sections is done by using at least first, second and third data reduction techniques on each said portion, to obtain first, second and third results, and to count said first, second and third results, and to establish frequently occurring sections when all of said first second and third results have a frequency of occurrence greater than a specified amount.

45. An apparatus as in claim 38, wherein said portion of data at includes a portion of the network payload.

46. An apparatus as in claim 40, wherein said module maintains a first list of unassigned addresses in said memory; forms a second list of sources that have sent to addresses on said first list; and comparing a current source of a frequently occurring section to said second list.

47. An apparatus as in claim 46, wherein said module data reduces information prior to storing in said list.

48. An apparatus as in claim 40, wherein said module operates to first monitor a first content sent to a destination;

second monitor a second content sent by said destination; and

determine a correlation between said first content and said second content as said additional test.

49. An apparatus as in claim 48, wherein said first monitoring comprises monitoring multiple destinations, and said second monitoring comprises monitoring multiple destinations during a different time period than said first monitoring.

50. An apparatus as in claim 49, wherein said first and second monitoring comprises data reducing information about said destinations, and storing at least one table in said memory about said data reduced information.

51. An apparatus as in claim 45, further comprising a data portion module that obtains a specified portion of data from the network.

52. An apparatus as in claim 46 wherein said portion of data further includes a portion of a network header.

53. An apparatus as in claim 47, wherein said portion of a network header is a port number indicating a service requested by a network packet.

54. An apparatus as in claim 46, wherein said portion of data comprises a first subset of a network packet including payload and header and wherein said data portion module further obtains a second subset of the same network packet for subsequent analysis.

55. An apparatus as in claim 54, wherein said data portion module forms a plurality of portions from each network packet, each of said plurality of portions comprising a specified subset of the network packet.

56. An apparatus as in claim 36, further comprising forming a plurality of portions from each network packet, each of said plurality of portions comprising a continuous portion of payload, and information indicative of aport number requested by a network packet.

57. An apparatus as in claim 36, further comprising:

first and second hash generators, respectively forming first and second hash functions of said portions;

a first counter, with a plurality of stages, connected such that respective stages of said counter are incremented based on said first hash function;

a second counter, with a plurality of stages, and connected such that respective stages of said counter are incremented based on said first hash function.

58. An apparatus as in claim 57, further comprising a module that checks said one of said stages of said first counter and said one of said stages of said second counter

against a threshold, and identifies said portion as frequent content only when both said one of said stages of said first counter and said one of said stages of said second counter are both above said threshold.

59. An apparatus as in claim 58, further comprising a frequent content buffer table storing specified frequent content.

60. An apparatus as in claim 59, further comprising at least a third counter, and a third hash generator, taking a third hash of said portion, and incrementing a stage of said third counter based on said third hash, where said module identifies said portion as frequent content only when all of said stages of each of said first, second and third counters are each above said threshold.

61. An apparatus as in claim 60, wherein said signature generator includes a sliding window portion that first obtains said portion by taking a first part of the message, and subsequently obtains said portion by taking a second part of the message.

62. A apparatus as in claim 61, wherein at least one of said hash functions is an incremental hash function.

63. An apparatus as in claim 38, wherein said signature generator operates to form a hash function of at least one of the source or destination address, to form a hash value, first determine a unique number of said hash values, and second determine said one of source or destination numbers based on said first determine.

64. An apparatus as in claim 63, wherein said count carried out by said signature generator further comprises scaling the hash value prior to said second determine.

65. A apparatus as in claim 63, wherein said scaling comprises scaling by a first value during a first counting session, and scaling by a second value during a second measurement interval.

66. An apparatus as in claim 36, wherein said memory stores a list of computers on the network, and stores an update level for each of said computers indicating which of said computers is susceptible to a specified kind of attack, and a module which monitors for said kind of attack

only when the message is directed for a computer which is susceptible to said kind of attack.

67. An apparatus of claim 66 where said module checks comprises checking for a message that attempts to exploit a known vulnerability to which a computer is vulnerable, as said specified attack.

68. An apparatus as in claim 67, wherein said module checks for a field that is longer than a specified length.

69. A method, comprising:

monitoring network content on a network, and obtaining at least a portion of data on said network;

data reducing said portion of data using a data reduction function which reduces said portion of data to a reduced data portion in repeatable manner, such that each portion which has the same content is reduced to the same reduced data portion;

analyzing said reduced data portion to find network content which repeats a specified number of times, and to establish said network content which repeats said specified number of times as frequent content;

identifying address information which includes at

least one of a source information or destination information for sources and/or destinations, of said frequent content, and determining if a number of sources and/or destinations for said frequent content is increasing; and

identifying the frequent content as associated with a network attack, based on said identifying.

70. A method as in claim 69, wherein said monitoring network content comprises obtaining both a portion of data on the network, and a portnumber indicating a service requested by a network packet.

71. A method as in claim 70, wherein said obtaining a portion of network data comprises defining a window which samples a first portion of network data at a first time defined by a position of the window, and sliding said window to a second position at a second time which samples a second portion of said network data that has a specified offset from the first portion.

72. A method as in claim 71, wherein said data reduction function is a hash function.

73. A method as in claim 72, wherein said data reduction function is an incremental hash function.

74. A method as in claim 69, wherein hash function is used in a scalable configuration.

75. A method as in claim 69, wherein said identifying comprises second data reducing said address information using a data reduction function, and maintaining a table of data reduced address information.

76. A method as in claim 75, wherein said second data reducing comprises hashing said address information.

77. A method as in claim 69, further comprising testing contents of the network packet associated with the frequent content to determine the presence of code in said contents.

78. A method as in claim 77, wherein said testing contents comprises determining an opcode in said contents, determining a length of the opcode, and looking for another opcode at a location within said contents based on said length.

79. A method as in claim 69, further comprising monitoring for scanning of addresses associated with said frequent content.

80. A system, comprising:

a signature generator, monitoring network content to obtain at least a portion of data from said network, and to data reduce said portion according to a data reduction function which reduces said portion to a reduced data portion in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion;

a memory, storing said reduced data portion;

wherein said signature generator counts a number of said reduced data portions and establishes said reduced data portion as frequent content based on said counting, and produces information indicative of said reduced data portion; and

an intrusion detection system, operating to protect a network against attacks, said intrusion detection system receiving information from said signature generator indicative of said frequent content, and using said information to monitor against said attacks.

81. A system as in claim 80, wherein said intrusion detection system is coupled to only one of said signature generators.

82. A system as in claim 80, wherein said intrusion detection system receives input from multiple different ones of said signature generators.

83. A system as in claim 80, wherein said memory also stores a list of computers on a local network, and an update level for said computers, and wherein said intrusion detection system monitors only for attacks based on the update level.

84. A system as in claim 80, wherein said signature generator also includes a part which monitors for an increasing number of address is associated with network packets that includes said frequent content, wherein said addresses include at least one of sources and/or destinations.

85. A system as in claim 84, wherein said addresses monitored by said signature generator also include a port 21 associated with said sources and/or destinations.

86. A system as in claim 84, wherein said signature generator operates to scale the counter by a first amount at a first time and by a second amount at a second time, to determine an increasing infection level.

87. An apparatus comprising:

an entry device, having a connection to a network, to obtain a portion of data from the network, operating to carry out a data reduction on said data portion to reduce said data portion to a reduced data portion in a repeatable manner;

a memory, storing said reduced data portions; and

a signature generator that operates to generate signatures that are used to detect common elements within said reduced data portion, said analyzing reviewing for common content indicative of a network attack.